Troubleshooting Guide

iVIEW

# iVIEW Suite
## Version 7.1

RADVISION®
Delivering the Visual Experience®

# NOTICE

© 2000-2009 RADVISION Ltd. All intellectual property rights in this publication are owned by RADVISION Ltd and are protected by United States copyright laws, other applicable copyright laws and international treaty provisions. RADVISION Ltd retains all rights not expressly granted.

This publication is RADVISION confidential. No part of this publication may be reproduced in any form whatsoever or used to make any derivative work without prior written approval by RADVISION Ltd.

No representation of warranties for fitness for any purpose other than what is specifically mentioned in this guide is made either by RADVISION Ltd or its agents.

RADVISION Ltd reserves the right to revise this publication and make changes without obligation to notify any person of such revisions or changes. RADVISION Ltd may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this publication, it is furnished under a license agreement included with the product as a separate document. If you are unable to locate a copy, please contact RADVISION Ltd and a copy will be provided to you.

Unless otherwise indicated, RADVISION registered trademarks are registered in the United States and other territories. All registered trademarks recognized.

GoAhead WebServer is used by permission from GoAhead Software, Inc. GoAhead WebServer is used by permission from GoAhead Software, Inc. Copyright © 2006 GoAhead Software, Inc. All Rights Reserved.

For further information contact RADVISION or your local distributor or reseller.

iVIEW Suite version 7.1, December 2009

Publication 3

http://www.radvision.com

# CONTENTS

## *About This Manual*


Related Documentation v
Feedback v


## *Troubleshooting*


How to Resolve Browser Authentication Issues 2
- Recognizing a Local Intranet Site 2
- Enabling Single Sign-on 2
- Configuring iVIEW Outlook Add-in for Single Sign-on 2

How to Resolve iVIEW Outlook Add-in Configuration Issues 3
- Connecting the iVIEW Outlook Add-in to iCM 3
- Disabling Pop-up Messages 3

How to Collect Logs 4
- Collecting iVIEW Suite Logs 4
- Collecting SCOPIA Desktop Logs 4

How to Resolve User Experience Issues 4
- Enabling Internet Explorer Pop-up Blocker 4
- Navigating Between Pages 5
- Configuring Maximum Time Period for Recurring Meetings 5
- Correcting Web Page and Pop-up Window Display 5

How to Resolve Administration Issues 5
- Database Unavailable 5
- Using Double-Byte Characters in the MCU Service Template 6
- Configuring Terminal Area Codes 6
- Assigning DID Numbers 6

How to Resolve IVR Issues 7
- Resolving Virtual Service Issue 7

Resolving Video IVR Issue 8
Resolving Auto Route Incoming Calls Issue 9
Resolving a Port Conflict 10
Resolving a Scheduling Failure 10
Resolving a Failed Terminal Invitation 12
Resolving a Meeting Creation Failure 13
Synchronizing SCOPIA Desktop Server with iVIEW Suite 14
Updating the IP Address on the Streaming Server 15
Changing IP Address of the SCOPIA Desktop Server 16
Recording Does Not Start Automatically 17

# About This Manual

The iVIEW Suite Troubleshooting Guide provides information for administrators about iVIEW Suite installation, configuration and the user interface. It includes detailed procedures about performing administrator-related tasks.

## Related Documentation

The iVIEW Suite documentation set is available on the RADVISION Utilities and Documentation CD-ROM supplied with the product and includes manuals and online helps. The manuals are in PDF format.

**Note** You require Adobe Acrobat Reader version 6.0 or later to open the PDF files. You can download Acrobat Reader free of charge from www.adobe.com.

## Feedback

The team at RADVISION constantly endeavors to provide accurate and informative documentation. If you have comments or suggestions regarding improvements to future publications, we would value your feedback.

Please send your comments to doc_comments@radvision.com.

We thank you for your contribution.

# TROUBLESHOOTING


- How to Resolve Browser Authentication Issues on page 2
- How to Resolve iVIEW Outlook Add-in Configuration Issues on page 3
- How to Collect Logs on page 4
- How to Resolve User Experience Issues on page 4
- How to Resolve Administration Issues on page 5
- How to Resolve IVR Issues on page 7
- Resolving a Port Conflict on page 10
- Resolving a Scheduling Failure on page 10
- Resolving a Meeting Creation Failure on page 13
- Resolving a Failed Terminal Invitation on page 12

# How to Resolve Browser Authentication Issues

## Recognizing a Local Intranet Site

### Symptom

The browser does not recognize iCM as a local Intranet site and an authentication window appears.

### Recommended Action

- Provide users with a link to iVIEW Suite that includes the necessary fully qualified domain name (FDQN), rather than only the iCM IP address.
- Configure the browser for the user so that iCM is a local Intranet site.

## Enabling Single Sign-on

### Symptom

iVIEW Suite web pages always require that you enter a user name and password.

### Recommended Action

Use Single Sign-on (SSO). SSO enables users to access iVIEW Suite web pages without having to enter a user name or password. Users are authenticated transparently using domain account and password credentials.

To enable Single Sign-on, during installation select the **Single Sign-on** check box. You must also add the iVIEW Suite host server to the trusted site of the client browser.

## Configuring iVIEW Outlook Add-in for Single Sign-on

### Symptom

iCM authentication fails when working with SSO and iVIEW Outlook Add-in.

### Recommended Action

Go to **Tools > Options > iVIEW Suite Meetings**. In the Outlook options, make sure the User ID, Password, and Organization fields are blank.

iCM automatically performs authentication using the domain account/password credentials.

# How to Resolve iVIEW Outlook Add-in Configuration Issues

## Connecting the iVIEW Outlook Add-in to iCM

### Symptom

The iVIEW Outlook Add-in fails to connect to iCM.

### Recommended Action

After installing the iVIEW Outlook Add-in, go to **Tools > Options > iVIEW Suite Meetings** and enter the URL of your server in the Web Site field.

## Disabling Pop-up Messages

### Symptom

The standard Microsoft Outlook 2003 pop-up message warning that another application is trying to access Outlook information appears.

### Recommended Action

Use the new registry key

HKEY_CURRENT_USER\Software\Policies\Microsoft\Security\CheckAdminSettings

for the Outlook client machine, and then set the value to 1.

---

**Note** To disable the pop-up message from the exchange-server side, refer to Microsoft documentation.

---

Meetings scheduled from iVIEW Outlook Add-in use the meeting organizer time zone setting from iVIEW Suite. Time zone settings on the work station of a Meeting Organizer should match the settings in iVIEW Suite. You can change time zone settings in iCM in My Profile.

---

**Note** We recommend that meetings created via the iVIEW Outlook Add-in contain no more than 100 participants.

---

# How to Collect Logs


- Collecting iVIEW Suite Logs on page 4
- Collecting SCOPIA Desktop Logs on page 4


## Collecting iVIEW Suite Logs

For information about collecting logs in iVIEW Suite, refer to the Administrator Guide for iVIEW Suite Release 7.0.

## Collecting SCOPIA Desktop Logs

**Procedure**

1. Access the SCOPIA Desktop Server.
2. Click the Conference Server icon on the taskbar to view the log in the Console window.
3. If necessary, save the log files located at these locations:

- C:\Program Files\CiscoRadvision\Cisco Unified Videoconferencing DesktopSCOPIA Desktop\ConfSrv\cs.log
- C:\Program Files\Radvision\SCOPIA Desktop\logs*.xml
- C:\Program Files\SCOPIA Desktop\tomcat\logs\stdout.log, stderr.log

# How to Resolve User Experience Issues

## Enabling Internet Explorer Pop-up Blocker

### Symptom

Internet Explorer Pop-up Blocker is inactive.

### Recommended Action

If you are using Microsoft Windows XP SP2 or Windows 2003 Service Pack 1, to enable Internet Explorer Pop-up Blocker, add the iCM site to the list of allowed sites. To do this, go to **Tools > Internet Options > Privacy > Pop-up Blocker Settings**, and then add the iCM site.

### Navigating Between Pages

**Symptom**

Internet Explorer browser navigation buttons (Back, Forward and Refresh) do not work correctly in the iVIEW Suite user interface.

**Recommended Action**

Use the Next and Back buttons in iVIEW Suite to navigate between pages.

### Configuring Maximum Time Period for Recurring Meetings

**Symptom**

You want to schedule recurring meetings for a period longer than that allowed in the iVIEW Suite Web user interface.

**Recommended Action**

Use the iVIEW Suite Configuration Tool to schedule recurring meetings for up to 730 days.

### Correcting Web Page and Pop-up Window Display

**Symptom**

Some Web pages and pop-up windows do not display normally.

**Recommended Action**

Set the screen resolution to a standard resolution such as 800 x 600 pixels or 1024 x 768 pixels. The minimum recommended resolution is 800 x 600 pixels and the recommended font size is Normal or Large.

## How to Resolve Administration Issues

### Database Unavailable

**Symptom**

No database is available when iVIEW Suite is initially started.

**Recommended Action**

Restart the service when the database is ready. If the connection between the database and iVIEW Suite is lost after initially starting iVIEW Suite, iVIEW Suite works normally when the database is operating.

## Using Double-Byte Characters in the MCU Service Template

### Symptom

Unicode and other double-byte characters (such as Chinese, Japanese, Korean, and Hebrew characters) cause device exception in MCU service template Name, Description, Terminal Name and Gateway Service Prefix fields.

### Recommended Action

Use only ASCII text in these fields.

## Configuring Terminal Area Codes

### Symptom

Terminal area codes are incorrectly defined.

### Recommended Action

Do not include domestic long-distance prefixes in terminal area codes.

## Assigning DID Numbers

### Symptom

Cannot change Direct Inward Dialing (DID) numbers

### Recommended Action

DID numbers are assigned on a per-endpoint basis rather than on a per-meeting basis. This is an internal configuration that cannot be changed via the Configuration Tool or the iVIEW Suite Web interface. To manually change the host name, perform the following procedure.

**Procedure**

1. Go to **C:\Program Files\RADVISION\iVIEW Suite\iCM\jboss\bin** where C is the local drive.
2. Make a backup copy of the vcs-config.xml file.
3. Open the vcs-config.xml file with a text editing tool and modify the <host-url> element to the required value.
4. Save the file in the text editor.
5. Restart iVIEW Suite.

# How to Resolve IVR Issues


- Resolving Virtual Service Issue on page 7
- Resolving Video IVR Issue on page 8
- Resolving Auto Route Incoming Calls Issue on page 9


## Resolving Virtual Service Issue

### Symptom

If iVIEW Suite is in the standalone mode and a user is configured with a virtual services prefix only on iVIEW Suite, a call cannot be routed to Video IVR when the user calls a virtual conference ID.

### Recommended Action

**Procedure**

1. Login to Enhanced Communication Server.
2. Navigate to **Gatekeeper > Endpoints >Endpoints** tab.
3. Click **Add Predefined**.
4. Configure settings as follows:
   - Endpoint type: Terminal
   - Registration IP: 127.0.0.1 Port: 1719
   - Call signaling IP: 127.0.01 Port: 1719
   - Aliases:
     - Value: Virtual Services; Type: Name
     - Value: Your auto virtual services prefix number; Type: Phone number
5. Click **Upload**.
6. Navigate to **Gatekeeper > Services > Services** tab.
7. Click **Add**.
8. Configure settings as follows:
   - Prefix: Your auto virtual services prefix number
   - Prefix type: phone number
   - Description: Virtual Services
   - Conference Hunting: Enabled
   - Global Service: No
   - Allow access for:

- In-zone non-predefined endpoints: enabled
- Out-of-zone endpoints: enabled

9 Click **Upload**.

## RESOLVING VIDEO IVR ISSUE

### Symptom

If iVIEW Suite is in a standalone mode and a user is configured with an auto-attendant number on iVIEW Suite only, a call to the auto-attendant number is not routed to Video IVR.

### Recommended Action

**Procedure**

1 Login to Enhanced Communication Server.
2 Navigate to **Gatekeeper** > **Endpoints** >**Endpoints** tab.
3 Click **Add Predefined**.
4 Configure settings as follows:
   - Endpoint type: Terminal
   - Registration IP: 127.0.0.1 Port: 0
   - Call signaling IP: 127.0.01 Port: 0
   - Aliases:
     - IVR Number; Type: Name
     - Your auto attendant number; Type: Phone number
5 Click **Upload**.
6 Navigate to **Gatekeeper** > **Services** > **Services** tab.
7 Click **Add**.
8 Configure settings as follows:
   - Prefix: Your auto attendant number
   - Prefix type: phone number
   - Description: End Point
   - Conference Hunting: Enabled

- Global Service: No
- Allow access for:
  - In-zone non-predefined endpoints: enabled
  - Out-of-zone endpoints: enabled

9 Click **Upload**.

## Resolving Auto Route Incoming Calls Issue

### Symptom

If iVIEW Suite is in the standalone mode and a user is configured with auto route incoming calls only on iVIEW Suite, a call cannot be routed to Video IVR when the user calls an auto route incoming call number.

### Recommended Action

**Procedure**

1 Login to Enhanced Communication Server.
2 Navigate to **Gatekeeper** > **Endpoints** >**Endpoints** tab.
3 Click **Add Predefined**.
4 Configure settings as follows:
   - Endpoint type: Terminal
   - Registration IP: 127.0.0.1 Port: 5
   - Call signaling IP: 127.0.01 Port: 5
   - Aliases:
     - Value: Routing Number; Type: Name
     - Value: Your auto route incoming calls number; Type: Phone number
5 Click **Upload**.
6 Navigate to **Gatekeeper** > **Services** > **Services** tab.
7 Click **Add**.
8 Configure settings as follows:
   - Prefix: Your auto route incoming calls number
   - Prefix type: phone number
   - Description: Virtual Services

- Conference Hunting: Enabled
- Global Service: No
- Allow access for:
  - In-zone non-predefined endpoints: enabled
  - Out-of-zone endpoints: enabled

9 Click **Upload**.

## RESOLVING A PORT CONFLICT

### Symptom

A port conflict occurs when you try to install or run certain applications.

### Recommended Action

Ensure that ports 11098 and 11099 are free. Run the “netstat” command in the DOS window to determine which applications (if any) occupy ports 11098 and 11099.

## RESOLVING A SCHEDULING FAILURE

### Symptom

In iCM, in My Meetings or Meeting Monitoring, on the Current tab, if Failed appears, if you click Failed, the message that opens reads: “Unable to create the meeting as scheduled. Please check your meeting settings.”

### Recommended Action

A scheduling failure may occur if a meeting type is downloaded, and then the meeting type is changed on the MCU but the iCM does not update the meeting types.

**Procedure**

1. To confirm that the reason for the failure is an incompatible meeting type, select **Admin > Meeting Types** and click **Download**.
2. If the meeting type that you specified appears in the Meeting Types (Service) Conflicts list, the reason for the scheduling failure is, at least in part, an incompatible meeting type.

**Note** If a meeting is created even though the specified meeting type is incompatible, there may be resource-calculation errors.

3. To resolve the conflict, repeat the download of the meeting type you require.

### Recommended Action

If actual MCU resources are changed after the MCU is added in iCM but iCM does not update or synchronize the actual MCU information, then the result may be an incompatible MCU.

**Procedure**

1. To determine which MCU is actually assigned to the meeting, select **Admin > Resource Management > MCU**.
2. Click the required MCU in the MCU column on the Current tab.
3. In the Modify MCU window, click **Synchronize**.

   The MCU profile is updated.
4. Make sure the MCU registered gatekeeper is configured correctly.
5. Make sure the connection configuration in **Admin > Network Management > IP Topology** is correct.

**Note** The Network Management section is hidden by default in iCM. Use the iCMConfiguration Tool to change default settings in the user interface.

# Resolving a Failed Terminal Invitation

### Symptom

You are not able to invite a terminal to a meeting.

### Possible Cause

Incompatible gatekeeper registration. The MCU may be registered to a gatekeeper that is different than the one specified in the MCU profile in iCM.

### Recommended Action

**Procedure**

1. In the MCU section of the SCOPIA MCU application, check that the ECS that is listed is the same as the one designated in iCM.
2. If the gatekeeper is not the same, then in iCM, select the same gatekeeper to which the MCU is registered.

### Possible Cause

Authorization failure. ECS version 4.1.5.0 or later allows multiple iCM to connect as authorizer. However, if multiple iCM authorizes a single ECS, the iCM/ECS authorization logic does not work.

### Recommended Action

Ensure that each ECS has only one iCM as its authorizer. If multiple iCM authorizes a single ECS, remove all other iCM authorization connections, and then restart ECS. Only after this does the remaining iCM work with this ECS properly in authorization mode.

**Note** iCM initiates the authorization connection to the ECS. Ensure that the ECS server SNMP Community names are set correctly in the iCM user interface.

### Possible Cause

Unconnected IP location (at Network Management > IP Topology) for the MCU and a terminal.

If a meeting is set up on the MCU that belongs to a specific location defined at Network Management > IP Topology, a terminal is invited to a different location, the location to which the MCU is assigned may not be able to connect to the location to which the terminal is assigned.

**Procedure**

1. In iCM, on the IP Topology tab, check that there is a link between the two different locations.
2. Make sure that if there is a connection, that Bandwidth and Location are correctly defined.
3. Alternatively, assign the MCU and the terminal to the same location.
4. Make sure that the gatekeeper that the terminal is assigned to is in Authorization Mode.

**Note** Cascading is set up in iCM in the Network Management section, on the IP Topology tab. If the IP Topology tab is hidden, in the iVIEW Suite Configuration Tool, in System Configuration > UI Settings, check **IP Topology** to activate the IP Topology tab.

## Resolving a Meeting Creation Failure

### Symptom

A meeting is successfully scheduled but cannot actually be created.

**Procedure**

1. Make a point-to-point call.
2. Ensure that the call is successful from within iCM. A successful point-to-point call indicates that the ECS and iCM are configured correctly.
3. Create an endpoint-initiated MCU conference. If the endpoint connects, the MCU, ECS and iCM are configured properly.Schedule a meeting in iCM. If the meeting is scheduled successfully, wait for the meeting to start. If the meeting starts successfully, dial into the meeting using an endpoint.

### Recommended Action

In the event that the troubleshooting procedures in this section do not resolve a meeting creation or meeting invitation issue, use the procedure in this section.

**Procedure**

1. Attempt the same meeting creation or invitation directly on the MCU without using the iCM.
2. If the same meeting creation or invitation does not succeed directly on the MCU, restart the MCU.
3. If restarting the MCU does not resolve the issue, contact your MCU service representative.

## SYNCHRONIZING SCOPIA DESKTOP SERVER WITH iVIEW SUITE

### Symptom

The Directory Status - iVIEW Suite tab displays the synchronization error.

### Recommended Action

Perform the procedure.

**Procedure**

1. Select the link on the Directory Status - iVIEW Suite tab.

   The Directory tab opens.
2. Select the **Synchronize** button.

# Updating the IP Address on the Streaming Server

## Symptom

The SCOPIA Desktop Status tab indicates that the Streaming Server is not connected. If you select the Streaming Server indicator, this error is displayed: “5003 Access denied error from proxy”.

## Recommended Action

When the Streaming or Recording components of SCOPIA Desktop are installed on their own server, separately from the SCOPIA Desktop Server, they are configured with the IP address of the SCOPIA Desktop Server which is allowed to connect to them. If the IP address of the SCOPIA Desktop Server changes, you need to update it on the Streaming and Recording Servers.

**Procedure**

1. From the Start menu, choose **Programs** > SCOPIA Desktop > **TCP Proxy Configuration**.
2. Run the listServers command to display the address of the SCOPIA Desktop Server which is allowed to access the Streaming or Recording Server.
3. If the SCOPIA Desktop Server address is incorrect, run the removeServer command to remove it.
4. Run the addServer command to add the correct address.
5. Follow on-screen directions to complete the procedure.

# Changing IP Address of the SCOPIA Desktop Server

### Symptom

The SCOPIA Desktop Status tab indicates that the SCOPIA Desktop Server is not connected.

### Recommended Action

If the IP address of the server on which the SCOPIA Desktop Server is installed changes, you need to update SCOPIA Desktop Server components with its new IP address.

**Procedure**

1. Select **Start** > **Settings** > **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. From the list of programs, choose SCOPIA Desktop, and then **Change**. The Setup Wizard opens.
4. In the Welcome screen select **Next**.
5. In the Program Maintenance screen, choose **Modify**, and select **Next**.
6. In the Custom Setup screen, select **Next**.
7. In the SCOPIA Desktop Serial Key screen, select **Next**.
8. In the SCOPIA Desktop Network Configuration screen, select **Next**.
9. In the SCOPIA Desktop Hostname Configuration screen, select **Next**.
10. In the SCOPIA Desktop Recording Configuration screen, select **Next**.
11. Select **Install**.

# Recording Does Not Start Automatically

## Symptom

iVIEW Suite configured to work with the SCOPIA Desktop Server does not record virtual room meetings or scheduled meetings automatically, even though iVIEW Suite is configured to do so.

## Recommended Action

Verify that one of the following problems does not interfere with recording:

- There are not enough available recording ports on the SCOPIA Desktop at the time when the meeting is scheduled.
- There are not enough available recording ports on the SCOPIA Desktop at the time when the meeting is scheduled.
- The maximum number of simultaneous recordings is reached.

www.radvision.com

## About RADVISION

RADVISION (NASDAQ: RVSN) is the industry's leading provider of market-proven products and technologies for unified visual communications over IP and 3G networks. With its complete set of standards based video networking infrastructure and developer toolkits for voice, video, data and wireless communications, RADVISION is driving the unified communications evolution by combining the power of video, voice, data and wireless – for high definition video conferencing systems, innovative converged mobile services, and highly scalable video-enabled desktop platforms on IP, 3G and emerging next generation networks. For more information about RADVISION, visit www.radvision.com


USA/Americas
T +1 201 689 6300
F +1 201 689 6301
infoUSA@radvision.com

EMEA
T +44 20 3178 8685
F +44 20 3178 5717
infoUK@radvision.com

APAC
T +852 3472 4388
F +852 2801 4071
infoAPAC@radvision.com



This document is not part of a contract of license as may be expressly agreed RADVISION is registered trademarks of RADVISION, Ltd. All trademarks recognized. All rights reserved © 2009 RADVISION, Ltd.